

Mastering Blockchain

Third Edition

A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more

Imran Bashir

Packt

BIRMINGHAM - MUMBAI

Table of Contents

Preface	xv
Chapter 1: Blockchain 101	1
The growth of blockchain technology	1
Progress toward maturity	2
Increasing interest	5
Distributed systems	7
The history of blockchain and Bitcoin	8
The events that led to blockchain	9
Electronic cash	10
Blockchain	12
Blockchain defined	12
Blockchain architecture	14
Generic elements of a blockchain	16
Benefits, features, and limitations of blockchain	21
Types of blockchain	24
Consensus	29
Consensus mechanism	29
Types of consensus mechanisms	30
Consensus in blockchain	31
CAP theorem and blockchain	33
Summary	35
Chapter 2: Decentralization	37
Decentralization using blockchain	37
Methods of decentralization	41
Disintermediation	42
Contest-driven decentralization	42
Routes to decentralization	44
How to decentralize	44
Decentralization framework example	45
Blockchain and full ecosystem decentralization	45

Storage	46
Communication	46
Computing power and decentralization	47
Pertinent terminology	49
Smart contracts	49
Autonomous agents	49
Decentralized organizations	49
Decentralized autonomous organizations	50
Decentralized autonomous corporations	50
Decentralized autonomous societies	51
Decentralized applications	51
Platforms for decentralization	56
Ethereum	56
MaidSafe	56
Lisk	56
EOS	57
Innovative trends	57
Decentralized web	57
Decentralized identity	58
Decentralized finance (DeFi)	59
Summary	61
Chapter 3: Symmetric Cryptography	63
Working with the OpenSSL command line	63
Introduction	64
Cryptography	64
Cryptographic primitives	67
Keyless primitives	68
Symmetric cryptography	77
Data Encryption Standard (DES)	84
Advanced Encryption Standard (AES)	85
How AES works	85
An OpenSSL example of how to encrypt and decrypt using AES	86
Summary	89
Chapter 4: Public Key Cryptography	91
Mathematics	91
Modular arithmetic	91
Sets	92
Fields	92
Finite fields	92
Prime fields	92
Groups	92
Abelian groups	92
Rings	93
Cyclic groups	93

Order	93
Asymmetric cryptography	93
Integer factorization	95
Discrete logarithm	95
Elliptic curves	95
Public and private keys	96
RSA	96
Elliptic curve cryptography	98
Digital signatures	114
Cryptographic constructs and blockchain technology	121
Homomorphic encryption	121
Signcryption	122
Secret sharing	122
Commitment schemes	123
Zero-knowledge proofs	124
Different types of digital signatures	130
Encoding schemes	134
Applications of cryptographic hash functions	135
Summary	138
Chapter 5: Consensus Algorithms	139
Introducing the consensus problem	139
The Byzantine generals problem	140
Fault tolerance	141
State machine replication	142
FLP impossibility	143
Lower bounds on the number of processors to solve consensus	144
Analysis and design	145
Model	145
Processes	145
Timing assumptions	145
Classification	146
Algorithms	147
CFT algorithms	147
BFT algorithms	152
Choosing an algorithm	180
Finality	180
Speed, performance, and scalability	181
Summary	181
Chapter 6: Introducing Bitcoin	183
Bitcoin—an overview	183
The beginnings of Bitcoin	186
Egalitarianism versus authoritarianism	187
Bitcoin definition	188
Bitcoin—A user's perspective	189

Cryptographic keys	195
Private keys in Bitcoin	195
Public keys in Bitcoin	197
Addresses in Bitcoin	198
Transactions	202
The transaction lifecycle	202
The transaction data structure	203
Types of scripts	208
Coinbase transactions	212
Transaction validation	213
Transaction bugs	213
Blockchain	214
The genesis block	216
Mining	220
Tasks of the miners	220
Mining rewards	221
Proof of Work	221
The mining algorithm	221
The hash rate	223
Mining systems	224
Mining pools	226
Summary	228
Chapter 7: The Bitcoin Network and Payments	229
The Bitcoin network	229
Full client and SPV client	236
Bloom filters	236
Wallets	237
Non-deterministic wallets	238
Deterministic wallets	238
Hierarchical deterministic wallets	238
Brain wallets	238
Paper wallets	238
Hardware wallets	239
Online wallets	239
Mobile wallets	239
Bitcoin payments	241
Innovation in Bitcoin	243
Bitcoin Improvement Proposals	243
Advanced protocols	244
Segregated Witness	244
Bitcoin Cash	247
Bitcoin Unlimited	247
Bitcoin Gold	247
Bitcoin investment and buying and selling Bitcoin	248

Summary	249
Chapter 8: Bitcoin Clients and APIs	251
Bitcoin client installation	251
Types of clients and tools	252
Setting up a Bitcoin node	253
Setting up the source code	254
Setting up bitcoin.conf	254
Starting up a node in the testnet	255
Starting up a node in regtest	256
Experimenting further with bitcoin-cli	258
Using the Bitcoin command-line tool – bitcoin-cli	260
Using the JSON RPC interface	261
Using the HTTP REST interface	262
Bitcoin programming	263
Summary	264
Chapter 9: Alternative Coins	265
Introducing altcoins	265
Theoretical foundations	268
Alternatives to Proof of Work	269
Proof of Storage	271
Proof of Stake (PoS)	271
Proof of Activity (PoA)	272
Non-outsourcable puzzles	272
Difficulty adjustment and retargeting algorithms	273
Kimoto Gravity Well	274
Dark Gravity Wave	274
DigiShield	275
MIDAS	275
Bitcoin limitations	276
Privacy and anonymity	276
Extended protocols on top of Bitcoin	281
Colored coins	281
Counterparty	282
Development of altcoins	283
Consensus algorithms	283
Hashing algorithms	283
Difficulty adjustment algorithms	284
Inter-block time	284
Block rewards	284
Reward halving rate	284
Block size and transaction size	284
Interest rate	284
Coinage	284
Total supply of coins	285

Token versus cryptocurrency	285
Initial Coin Offerings (ICOs)	286
ERC20 standard	287
Summary	288
Chapter 10: Smart Contracts	289
History	289
Definition	290
Ricardian contracts	293
Smart contract templates	297
Oracles	299
Software and network-assisted proofs	301
Hardware device-assisted proofs	302
Types of blockchain oracles	304
Blockchain oracle services	307
Deploying smart contracts	308
The DAO	309
Summary	310
Chapter 11: Ethereum 101	311
Ethereum – an overview	311
The yellow paper	313
Ethereum – a user's perspective	315
The Ethereum network	318
The mainnet	318
Testnets	318
Private nets	318
Components of the Ethereum ecosystem	319
Keys and addresses	320
Accounts	321
Transactions and messages	322
Ether cryptocurrency/tokens (ETC and ETH)	332
The Ethereum Virtual Machine (EVM)	333
Execution environment	335
The machine state	336
The iterator function	337
Smart contracts	338
Native contracts	338
Summary	340
Chapter 12: Further Ethereum	341
Blocks and blockchain	341
The genesis block	343
The block validation mechanism	344
Block finalization	345
Block difficulty mechanism	346

Gas	347
Fee schedule	348
Wallets and client software	348
Wallets	349
Geth	349
Eth	349
Parity	349
Trinity	349
Light clients	350
Installation and usage	350
MetaMask	359
Nodes and miners	370
The consensus mechanism	372
Forks in the blockchain	373
Ethash	373
APIs, tools, and DApps	379
Applications (DApps and DAOs) developed on Ethereum	380
Tools	380
Geth JSON RPC API	380
Supporting protocols	383
Whisper	383
Swarm	383
Programming languages	384
Runtime bytecode	385
Opcodes	386
Summary	386
Chapter 13: Ethereum Development Environment	387
Overview	388
Test networks	388
Components of a private network	389
Network ID	392
The genesis file	393
Data directory	394
Starting up the private network	395
Mining on the private network	398
Remix IDE	407
MetaMask	413
Using MetaMask and Remix IDE to deploy a smart contract	415
Adding a custom network to MetaMask and connecting Remix IDE with MetaMask	415
Importing accounts into MetaMask using keystore files	417
Deploying a contract with MetaMask	420
Interacting with a contract through MetaMask using Remix IDE	424
Summary	430

Chapter 14: Development Tools and Frameworks	431
Languages	432
Compilers	433
The Solidity compiler	433
Tools and libraries	437
Node.js	437
Ganache	439
Frameworks	442
Truffle	442
Drizzle	444
Embark	444
Brownie	444
Waffle	445
Etherlime	445
OpenZeppelin	445
Contract development and deployment	445
Writing smart contracts	445
Testing smart contracts	446
Deploying smart contracts	447
The layout of a Solidity source code file	447
Version pragma	447
Import	447
Comments	447
The Solidity language	448
Variables	448
Data types	450
Control structures	454
Events	455
Inheritance	456
Libraries	457
Functions	457
Error handling	462
Summary	462
Chapter 15: Introducing Web3	463
Exploring Web3 with Geth	463
Contract deployment	464
POST requests	472
Interacting with contracts via frontends	473
The HTML and JavaScript frontend	473
Interacting with contracts via a web frontend	475
Development frameworks	483
Using Truffle to develop a decentralized application	484
Using Truffle to test and deploy smart contracts	496
Deployment on decentralized storage using IPFS	503

Summary	508
Chapter 16: Serenity	509
Ethereum 2.0—an overview	510
Goals	511
Main features	511
Roadmap of Ethereum	511
Development phases	512
Phase 0	512
Phase 1	520
Phase 2	522
Phase 3	522
Architecture	522
Summary	524
Chapter 17: Hyperledger	525
Projects under Hyperledger	526
Distributed ledgers	526
Libraries	529
Tools	530
Domain-specific	532
Hyperledger reference architecture	533
Hyperledger design principles	535
Hyperledger Fabric	537
Membership services	537
Blockchain services	538
Smart contract services	540
APIs and CLIs	540
Components	540
Applications on blockchain	542
Consensus in Hyperledger Fabric	545
The transaction lifecycle in Hyperledger Fabric	546
Fabric 2.0	547
Hyperledger Sawtooth	550
Core features	550
Consensus in Sawtooth	551
Transaction lifecycle	553
Components	554
Setting up a Sawtooth development environment	560
Prerequisites	561
Setting up a Sawtooth network	561
Summary	566
Chapter 18: Tokenization	567
Tokenization on a blockchain	568
Advantages of tokenization	568

Disadvantages of tokenization	570
Types of tokens	571
Fungible tokens	571
Non-fungible tokens	572
Stable tokens	573
Security tokens	574
Process of tokenization	574
Token offerings	575
Initial coin offerings	575
Security token offerings	576
Initial exchange offerings	576
Equity token offerings	576
Decentralized autonomous initial coin offering	576
Other token offerings	577
Token standards	578
ERC-20	578
ERC-223	579
ERC-777	579
ERC-721	579
ERC-884	579
ERC-1400	580
ERC-1404	580
Trading and finance	581
Financial markets	581
Trading	581
Exchanges	582
Orders and order properties	582
Components of a trade	583
Trade lifecycle	584
DeFi	585
Trading tokens	586
Regulation	586
Building an ERC-20 token	586
Pre requisites	587
Building the Solidity contract	587
Deploying the contract on the Remix JavaScript virtual machine	593
Adding tokens in MetaMask	605
Emerging concepts	612
Tokenomics/token economics	612
Token engineering	613
Token taxonomy	613
Summary	614
Chapter 19: Blockchain – Outside of Currencies	615
The Internet of Things	616

Internet of Things architecture	616
Benefits of IoT and blockchain convergence	619
Implementing blockchain-based IoT in practice	621
Government	637
Border control	638
Voting	640
Citizen identification (ID cards)	640
Health	641
Finance	642
Insurance	642
Post-trade settlement	643
Financial crime prevention	644
Payments	644
Cross-border payments	645
Peer-to-peer loans	645
Media	646
Summary	647
Chapter 20: Enterprise Blockchain	649
Enterprise solutions and blockchain	650
Success factors	651
Limiting factors	652
Slow performance	652
Lack of access governance	652
Lack of privacy	653
Probabilistic consensus	653
Transaction fees	653
Requirements	654
Privacy	654
Performance	655
Access governance	656
Further requirements	656
Enterprise blockchain versus public blockchain	659
Use cases of enterprise blockchains	660
Enterprise blockchain architecture	660
Network layer	661
Protocol layer	661
Privacy layer	662
Governance layer	662
Integration layer	662
Application layer	663
Security, performance, scalability, monitoring	663
Designing enterprise blockchain solutions	664
TOGAF	664
Architecture development method	665

Blockchain in the cloud	668
Currently available enterprise blockchains	669
Corda	670
Quorum	670
Fabric	670
Autonity	670
Comparison of main platforms	670
Enterprise blockchain challenges	672
Interoperability	672
Lack of standardization	672
Compliance	673
Business challenges	673
Corda	674
Architecture	674
CorDapps	677
Components	678
Corda development environment	683
Quorum	684
Architecture	685
Privacy manager	686
Cryptography used in Quorum	687
Privacy	687
Access control with permissioning	692
Performance	693
Pluggable consensus	694
Setting up Quorum with IBFT	694
Quorum Wizard	694
Cakeshop	697
Running a private transaction	698
Further investigation	702
Other Quorum projects	705
Remix plugin	705
Pluggable architecture	705
Summary	706
Chapter 21: Scalability and Other Challenges	707
Scalability	708
Blockchain planes	708
Methods for improving scalability	710
Privacy	719
Anonymity	719
Confidentiality	719
Techniques to achieve privacy	719
Security	727
Formal verification	727

Smart contract security	731
Other challenges	740
Interoperability	740
Lack of standardization	741
Post-quantum resistance	741
Compliance and regulation	742
Summary	743
Chapter 22: Current Landscape and What's Next	745
<hr/>	
Emerging trends	746
New implementations of blockchain technology	746
Technology improvements	747
Ongoing research and study	749
Innovative blockchain applications	752
Some debatable ideas	753
Areas to address	755
Regulation	755
Illegal activity	756
Privacy or transparency	757
Blockchain research topics	757
Smart contracts	757
Cryptographic function limitations	758
Consensus algorithms	758
Scalability	758
Code obfuscation	758
Blockchain and AI	759
The future of blockchain	760
Summary	761
Index	763
